Risk Appetite Assessment Algorithm - A Starting Point for Small And Medium Size Organisation for Understanding Information Security Requirements

UNIVERSITY OF TURKU
Department of Future Technologies
Master of Science in Technology Thesis
Security of Networked Systems
May 2020
NGEKEH PRISCA CHANA

Supervisors:
Dr. Antti Hakkala
Dr. Seppo Virtanen

UNIVERSITY OF TURKU
Department of Future Technologies

NGEKEH, PRISCA CHANA: Risk Appetite Assessment Algorithm

Master of Science in Technology Thesis, 53 p., 6 app. p.
Networked Systems Security
May 2020

Risk appetite is an important element of any effective risk management process. It is the foundation on which risk decisions are made, but unfortunately it is not often given the attention it deserves. This could be because of the lack of appreciation of its importance. Without a well-defined risk appetite analysis in place, it is very likely for an organization's risk assessment process to result in over- or under measured security solutions, or risk decisions that are not in line with the organization's business objectives. This thesis focuses on the importance of risk appetite assessment at an early stage of risk management process. Although risk management will be discussed in brief, our main focus is risk appetite.

This thesis examines the importance of risk appetite, the reasons why it should be given more attention in organizations, and presents a risk appetite assessment model that can be used by organizations to assess their businesses for an initial high-level description of their risk appetite: how much security is expected, where to focus security resources, etc. This general model can be adapted by small and medium sized organizations for decision making during their risk management process.

Towards the end of the thesis, a sample predictive analysis for an organization's risk appetite is presented. This model is built and adapted through a supervised machine learning algorithm which learns through experience from the trained data in order predicts the future risk appetite of an Organization. Though the accuracy of this prediction model is limited by the small data size, it can be seen that, risk appetite is inversely proportional to risk.

Keywords: Risk, Risk appetite, Information security, Risk Value, Algorithm.

Contents

List of figures

List of Tables

1 Introduction

There are over 400 different types of risk assessment tools available but really hard to find a risk appetite assessment tool. UC Risk Appetite Definition and assessment of Risk (UC RADAR) is one of the risk appetite assessment tool available but it focuses on environmental risk appetite. Risk appetite is appreciated by all but not applied in the risk management process. This might be caused by lack of clear defined steps on how to establish and used risk appetite or a risk appetite tools to help companies in their calculations.

Risk appetite is used in risk treatment process but it is not outline how it is been done. There are thousands of risk assessment methodologies but none of them considered risk appetite as one of the main steps. ISO31000 appreciate risk appetite but does not outline how it should be assessed (Edgerton, 2013). Challenges attributed to the calculation of risk appetite are due to, varying definition, different method of description/calculation and also, most organisations are unwilling to share their methodologies with other who are interested in risk appetite calculation (RIMS, 2009).

In this thesis, the next chapter (chapter two) introduces risk and risk appetite. It provides an overview of risk as a whole, IT risk in particular, with close attention on information security risk and the thesis problem. Chapter three is literature review. Here, we will contrast and compare what scholars have writing on risk appetite, advantages of risk appetite, developing risk appetite and factor affecting risk appetite. In chapter four, we introduce our proposed risk appetite assessment algorithm (solution to the thesis problem), providing a step by step approach - from requirements and design through assumptions, the algorithm, and constraints. Chapter five is where we are going to look at a case study. We will see how this algorithm could be implemented is this case study. In chapter six, we use machine learning algorithm to check risk appetite in our local businesses and chapter seven gives the conclusion to this thesis.

2 Risk

Risk is a word that is used in a variety of professional life areas such as health, insurance, and security. Risk in general terms is the total consequences of exercising vulnerability, taking into account the frequency of occurrence (Calder & Watkins, 2010). It could also be seen as the likelihood that a loss will occur (Gibson, 2015). Other definitions such as that of Hillson & Murray-Webster (2007), is “uncertainty that mater”. The point is, no matter what definition it takes, it is centred on uncertainty and consequences and therefore it is an important factor for the success of any business.

When risk is well managed, threats are reduced, opportunities increase and achievements of objectives are enhanced. This statement, at least theoretically is true but in reality, we usually don’t define enough principles, processes, or practical actions to achieve this success. One of these principles or processes is risk appetite. Risk appetite is an element of risk management. It has the potentials to influence great results in terms of consistency in decision making, and choosing control options that are well in-line with the business’s objectives (Hillson & Murray-Webster, 2007).

In this chapter, we will discuss risk appetite in the context of information security risk assessment. As we will find out, Information security is a sub-set of IT security and one of the most important security domains – due to the value of information to the success of organisations today.

2.1 Information security risk

Every organisation is faced with different types of risk. At a high level, we talk of organisational risk, then IT security risk with information security risk as a sub-set of IT security risk. Although the terms IT security and Information security risk are often interchanged, the formal is a broader concept and takes care of risk from any information technology tool or process while the latter focuses on risk to information only. That is, risk from tools, technologies, and procedures used for processing and protecting information.

According to Calder & Watkins (2010), security risk is defined as the possibility of threat exploiting vulnerabilities of assets and causing harm to an organisation. Organisations that uses technology to run and manage their sensitive or confidential information are exposed to threats such as viruses, DDoS attacks, and system failures. These threats will strive to exploit corresponding vulnerabilities on these technologies. Once this happens, we say a security breach has occurred. The likelihood that a system or technology will experience an attack that could compromised the availability, integrity and/or confidentiality of their information.

2.2 Information security risk management

Information is a very important asset to a company (Redman, 1998). Thus ensuring its confidentiality, availability and integrity is of high priority to most if not every organisation today. Organisations will usually define and implement processes, policies, standards, procedures, and controls just to protect this important asset. Technically, this is an attempt to managing risk to information as an asset. The process of managing risk related to information and information assets is referred to as Information security risk management (ISO27001, 2006). In general, this process could be defined in 3 main steps which are risk assessment, risk treatment and risk residual.

2.2.1 Risk Assessment

Risk assessment is the first and most important step of the risk management process. It is usually a combination of both risk analysis and risk evaluation. According to ISO27001 During risk assessment, the following takes place;

Firstly, identifying your assets: Here the organisation is expected to define their scope and identify assets within their scope. These assets could be tangible for instance data or intangible for instance reputation. Secondly, identify your legal and regulatory requirements: It is equally important for the organisation to identify legal and regulatory requirements that may affect the assets identified above. This is an important step as it would help in the valuation of assets. Thirdly, valuation of identified assets: Knowing the value of an asset will guide us identify

appropriate security method. Asset valuation scale could be in three or five levels depending on the organisation. The value of an assets depend on their importance to the organisation. Fourthly, threat and vulnerability identification: Involves the identification of threats and vulnerabilities relevant to identified assets. In the context of Information security, vulnerability is any weakness in technologies or controls protecting assets while threat is referred to as anything that has the potential to cause harm to the assets that is, exploit a vulnerability. This could be internally or externally, intentionally or unintentionally. For Example human error is an internal unintentional threat. Next, assessing the likelihood that a threat will exploit identified vulnerability: When threat and vulnerability meets, there is an incident. This is the point where identified threats and vulnerabilities are mapped. The scale for threat assessment could be low, medium, and high. The scale for vulnerability could be probable, possible and unlikely. Finally, risk calculation and evaluation: Two basic methods for evaluation are qualitative and quantitative. Calculations are done based on threat, vulnerabilities, and assets. Quantitative method ensures that the estimation of risk value is connected with numerical measurement and monetary value provided by the companies. Considering a company which has data, software, hardware, users and network topology as some of its assets, the quantitative risk calculation could be as shown in table 1 below.

Information Assets	Vulnerability (V) (scale of 1-3)	Threat (T) (scale of 1-3)	Likelihood of occurrence (L) (vulnerability x threat)	Assets Value (A) (scale of 1-3)	Risk value (R) (Likelihood of occurrence x asset value)	Risk rating (W) (scale of 1-27)
Data	3	3	9	3	21	High
Software	2	3	6	3	18	Medium
Hardware	2	2	4	1	4	Low
Users	3	3	6	2	12	Medium
Network topology	2	1	2	1	2	Low

Table 1: Quantitative Risk Analysis

R = (L).(A) Which is = (V.T).(A) and W = value from 1-27. Where: ≥ 20 is considered High, >10 < 20 is considered Medium, and ≤10 is considered Low.

Qualitative method does not use numerical data rather it uses description to present result. The risk assessment is done using judgment, experience and intuition as seen in table 2. Where we have a scale of 1 to 3, 1 = Low, 2 = medium, and 3 = High.

Information Assets	Vulnerability (V) (scale of 1-3)	Threat (T) (scale of 1-3)	Likelihood of occurrence (L) (vulnerability x threat)	Assets Value (A) (scale of 1-3)	Risk value (R) (Likelihood of occurrence x asset value)	Risk rating (W) (scale of 1-27)
Data	High	High	High	High	High	High
Software	Medium	High	Medium	High	Medium	Medium
Hardware	Medium	Medium	Low	Low	Low	Low
Users	High	High	Medium	Medium	Meduim	Medium
Network topology	Medium	Low	Low	Low	Low	Low

Table 2: Qualitative Risk Analysis.

2.2.2 Risk Treatment

After the risk assessment process is completed and the risks are identified and calculated, the next step is to treat the risks. The cost and likelihood of occurrence affects the treatment decision. There are four major categories of risk treatment: The first is Reduction: The risk could be reduce to acceptable level by using appropriate controls. This could be done by reducing the likelihood of exploiting vulnerability or reducing the impact of the risk when it occurs. The second is risk avoidance: This is when the organisation avoid any risk from occurring. This can be done by avoiding certain business activities such as online payments. The third is risk acceptance: There are some risk whose control might be difficult to identify or implementation or the cost might outweigh the benefit. In this case, the organisation might accept the risk and its consequences if risk occurs. When the organisation is unable to accept such risk, it could transfer the risk to a third party. And the forth is risk transfer: Risk could be transferred to insurance companies or outsourcing partners. The insurance company bear the responsibility of possible incident and loss. It is hard for insurance to cover the risk 100 percent because it is going to give some conditions and exclusions. Outsourcing partners

should be specialist in handling such risk. This does not completely eliminate all risk and might lead to the introduction of new risk (risk residual).

2.2.3 Risk residual

After risks controls have been implemented, there is still a certain level of risk left. This kind of risk is known as residual risk. It is practically impossible to completely eliminate risk but it could be reduced to an acceptable level. To Harris & Maymí (2016), there is no system with a 100% secured risk environment. When the residual risk is lower than the acceptable level of risk, it is good for the organisation. If it is higher than the acceptable level of risk, then the residual risk need to be reassessed. Residual risk is important to an organisation because, it helps organisation to know if the treatment is enough or not. (Landoll, 2011). Every step taken in the risk management process need to be documented for future reference.

In the above risk management process, risk appetite is not a defined step. ISO27001 is a well-known and used management process but does not lay emphasis on the importance of risk appetite. It does not also take risk appetite as one of the steps in risk management process. It talks about a predefined scale which is close to a risk appetite document but not mature enough. It should have been addressed from the start. If it was considered, it would have led to a better decision making and a much more effective risk process and true residual risk.
If we look closely to the risk management process described above, we would quickly realise the absence of a direct risk appetite consideration. Considering its significance, we would expect risk appetite to be a standalone option during risk assessment, as it's a key element that will greatly affect decision making during risk treatment. Unfortunately most risk tools and methodology are designed following the above process, with subtle differences. In the next chapter, we would exploit risk appetite in details, its definition, its importance and some literature review.

3 Risk Appetite

To Hillson & Murray (2012) risk appetite is an “internal drive to take risk in a given situation expressed via risk thresholds” while ISACA (2013) define risk appetite as the quantity of risk an organisation will accept in order to achieve its mission.

In general, as organisation’s risk varies, so too does risk appetite. There is therefore a need to determine separate risk appetite for each risk in an organisation including information risk. Leadership and culture plays a vital rule in determine an organisation's risk appetite. This is because, due to culture some leader turn to take very little risk and miss a lot of opportunities that might help in the growth and development of the company. Good cultures encourage leaders to take appropriate risk (PwC, 2017). As it turns out, organisations with higher risk appetite usually have the desire to engage more in risky actions. Organisations with low risk appetite are known to be highly concerned about business stability and regulatory requirements and will engage less in risky actions. For example, a None Profit Organisation will normally have a low risk appetite because it is more concerned about business stability whereas profit making organisation will prefer to have high risk appetite in order to have a higher profit (Gravelle, 2018).

To fully understand the underlined concept related to risk appetite, it is important we clarify the confusions that usually exist between some risk related terms such as risk capacity, risk threshold and risk appetite. Risk capacity is the maximum amount of risk an organisation can take considering its potentials and objective. Risk threshold falls within a company’s risk capacity and measures the risk appetite of a company in both upper and lower limits. While risk appetite is the desire to take risk in a given situation and is measured in risk threshold, it indicates the actual risk an organisation takes as illustrated in figure1 bellow (Hillson & Murray, 2012).

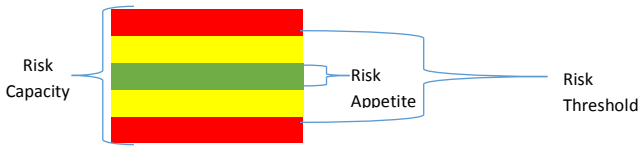

Fig 1. Risk Related Terms.

Risk appetite determination is a risk technique which have been seen as very useful. It helps association not to take risk more than their risk capacity (Fraser, Simkins & Narvaez, 2015). In the context of information security, risk appetite is an integral part of risk management process. Organisations need to know how much risk they will be willing to take as they pursue their information security objectives. In developing information security risk appetite for an organisation, a number of questions are considered. Such question should be designed to find out how much risk the organisation is willing to take and at what level the acceptable risk mirrors the organisation's business objectives and risk attitude. An organisation can determine it risk appetite by answering questions related to risk perception, risk exposure, risk culture, risk capacity, risk attitude and risk limits (Hillson, 2015).

3.1 Contrasting existing literature on subject

COSO (2012) said as organisations pursue their goals, they must encounter risk. McKay (2013) added that, companies with high risk appetite often have high objectives and vice versa. For RIMS (2009) Start-up companies usually have high risk appetite. While Susanto (2013) said the level of risk appetite of an organisation is related to the type of job and the objectives it seeks. Most organisations with high risk appetite are those seeking more reward.

According to Rittenberg & Martens (2012) there are three steps to determine risk appetite. Which are development of risk appetite, communication of risk appetite, monitoring and updating risk appetite. They also added that, there is no right risk appetite. The choice depend on the management. Hillson & Murray (2012) said that, there is no standard risk appetite statement for an organisation and that risk appetite need to be updated and monitored.

To Rittenberg & Martens (2012) it is the place of the management to develop the risk appetite while the board confirms it. Young & Coleman (2009) Board of directors need to take part in determine risk appetite. To Alix (2012) Risk appetite development should be done by board of directors and chief executive officers not only the chief risk officers. Hillson & Murray (2012) acknowledges that, risk appetite in most companies is decided by the board of directors and they align it with strategic goals. When developing risk response (risk treatment), risk appetite statement is taken into consideration. Every management have a level of desire for risk depending on the return but some managers will not want to take high risk and prefer low or average return. To Rittenberg & Martens (2012). When the risk appetite statement is done together with the shareholder, the interest of the shareholder is protected since it is taken into consideration.

Hillson & Murray (2012) said some organisations turn to ignore risk appetite but when risk appetite is not taken into consideration, organisation turn to suffer from more risk than anticipated (risk obesity). Rittenberg & Martens (2012) confirms this fact by saying that, some organisations are reluctant to the development of risk appetite. Organisations turns to take more risk when they fail to consider risk appetite. According to McKay (2013) not every organisation accepts risk appetite. But Chapman (2013) said an organisation's appetite for risk varies according to its objectives and culture. According to Hopkin (2014) though risk appetite is a very essential aspect of risk management, it is not easy to define and apply it in practice.

To Young, & Coleman (2009) in the banking sector, risk appetite and risk tolerance are not clearly understood and many people use these terms interchangeably. To Freund (2015) there is always a mix-up between the term risk appetite and risk tolerance

COSO (2004) emphasis on the important of risk appetite as an important element in enterprise risk management. Gravelle (2018) risk appetite is used in risk treatment process To RIMS (2009) organisation need to have good capacity to handle high risk

To Edgerton (2013) despite the importance of risk appetite, it is often neglected or not understood by risk managers and some organisations. Thus risk management team need to do more work when bringing in risk appetite. While to Freund (2015) Information security organisation hardly handle risk appetite effectively.

3.2 Advantages of Risk Appetite

There are several reasons why having a well-defined risk appetite is important to the success of any information security management program. With risk appetite in place, the security team in charge of risk management will be able to set clear goals and achieve these goals thus sustaining their business operations. As stated by Hillson & Murray (2012) when risk appetite for an organisation is in line with the operational, compliance and reporting objectives, the organisation is likely to meet its strategic goals.

Risk appetite enables information security management to regulate the amount of risk using risk threshold as a measuring scale during information security risk management. If the risk appetite is above risk threshold, the risk treatment needs to be implement to bring the risk back within the risk threshold (Tipton & Krause, 2010). Risk appetite gives information security management a clear guide to what amount and type of risk to take. (Freund, 2015).

Risk appetite help information security manager to effectively determine the right risk treatment. With risk appetite, the management will be able to make useful decisions such as which risk should be taken or not thus setting the risk boundaries. (Edgerton, 2013).

Risk appetite could also guide in the setting of strategic information security objectives. A good risk appetite analysis will help management not to consider risk that are not in-line with information security strategic objectives. Management will know the limit to which objectives has to be pursue. For management to decide on how much risk they are willing to take, it is a strategic decision. When the objectives goes beyond risk appetite level it should be terminated or adjusted.

When business set information security strategic objectives, the key risk needs to be identified and the appetite for each risk calculated for the management to decide if they would want to accept such risk or not (Smart & Creelman, 2013).

Risk appetite guide the allocation of resources where the risk is high, more resources are allocated to it and vice versa thus no waste is incurred. (Rittenberg & Martens, 2012).

To conclude, it is worth noting that, the above advantages can only be achieved if the information security risk appetite is well researched and developed. It is only when risk appetite is well defined and clearly communicated that it can improve business performance since management will be aware of the exiting risk and what type and amount to take.

3.3 Developing Risk Appetite

Considering the importance of risk appetite in the success of an organisation, it is vital that organisations, especially their information security team develop and establish a well-structured risk appetite for based-line decision making. The very first step is for the information security team to determine how much information risk they are ready to accept. Information security management could use previous information risk management report as a guide to make this decision. Otherwise, a comprehensive information risk assessment process could be used.

The information security team in charge could also develop an information security risk appetite statement. There is no standard risk appetite statement that an organisation must use but each organisation can developed its own. This statement needs to be owned, constantly updated and monitored so that it remains in-line with any changes in the objectives of the organisation. The information security risk appetite table is a good approach in the development of information security risk appetite. There are two tables associated with risk appetite which are the impact table and likelihood table.

Impact Table: Both internal and external stakeholders' interests should be consider in designing the impact table. This is because they greatly affect risk appetite decision making. For instance, customers trust must be maintained by preventing any breach in their private information. Thus risk appetite decision making most be in line with this interest. When the stakeholders are identified, their value drivers has to be also identified alongside. The value drivers helps in meeting up with the demands of stakeholders. When the value drivers are identified, the key risk indicators have to be identified from the selected value drivers. From key risk indicator, appropriate thresholds are established. For example if we consider a stake holder like customers, the interest of the customer is data privacy, the value driver will be prevention of data breach, key risk indicator will be lost of trust and customer, while the thresholds level could be between 1 to 10 customers.

Likelihood table: This table gives us the probability of an event occurring and can be measure in three or five scale depending on the company. Three scale measurement include medium, high and low. Qualitative or quantitative analyses methodology could be used in developing the risk appetite likelihood table.

Risk appetite table: Every event of information breach needs to be assessed and assigned a risk score. Risk scores are obtained from the product of impact and likelihood scores. Depending on the risk score, certain actions could be taken. Events with high risk needs immediate actions. For instance, consider a vulnerability associated with physical and environmental security such as unprotected information storage. If compromised the impact will be high depending on the type of information (Confidential, internal, and public). After the design of the risk appetite table, the risk appetite need to be validated, communicated and tested. Table 3 gives us a summary of a risk appetite decision table (Tipton & Krause, 2010).

Class of information	Impact value	Likelihood/ Frequency of occurrence	Impact	Action	Response time
Confidential	High	>5 a year	-Financial loss -Loss of customers -reputation damage	Accept the risk and use appropriate security measures in place such as strong encryption of the data	Immediately
Restructed	Medium	1- 5 a year	Financial loss -Loss of customers -reputation damage		Withine 5hrs
Internal use	Low	Onces a year	-Financial loss -reputaiton damage		Withine 3days
Public	Vary low	Frequently	No effect	No action	No action

Table 3. Sample Information Security Risk Appetite Table.

3.4 Factor Affecting Risk Appetite.

We will examine some of the factors influencing risk appetite that have been discussed in literature.

Existing risk profile: Risk profile is the evaluation of the company's readiness and ability to take risk. It outlines the number, types and effects of risks on a company. When the exiting risk profile shows that a particular risk occurs frequently, an organisation will have low appetite for such risk and if the risk hardly occurs there will be a high risk appetite to such risk (McKamey, 2018).

Risk propensity: it is the tendency for a person to take or avoid risk. Individual with high risk propensity will obviously have a high risk appetite and vice versa. Risk appetite comes from risk propensity and risk culture and is measured by risk threshold. Risk propensity plays a rule on risk appetite decision making. When important decisions take place under incomplete risk appetite information the management is bound to make wrong risk appetite decisions. Young people have high risk propensity than older poeple (wang, zhao, wenjing zhang and yu wang, 2015).

Risk culture: Believes and values of a defined set of people about information risk. When the culture is good, it promotes appropriate information risk appetite and vice versa thus aligning risk appetite with risk culture. Risk culture is very difficult to change but if change is necessary for effective information risk appetite, then the management must do it wisely (ERM, 2009).

Risk capacity: it is the maximum risk which an organisation can take in both upper and lower limits. The information security risk appetite should not exceed the risk capacity. If that happens then the risk appetite has to be re-analysed. When determine the risk capacity, the organisation need to know their ability to absorb possible losses. While assessing the risk capacity, the probability of the investments turning negative and the losses from the outcome should be taken into consideration (Andrew, 2018).

Risk thresholds: Since risk appetite is a desire and cannot be touch, risk thresholds is use as its external measuring instrument. Risk thresholds and tolerance could be used interchangeably. It indicates the upper and lower limits to acceptable risk. This is the amount of risk that an organization or company can accept. It is the measuring scale of risk appetite. In order to determine the risk threshold, the project managers have to schedule meetings and interviews with the stakeholders to find out their risk appetites. He/She analysing the uncertain events that can influence the projects both positively and negatively before calculating the risk threshold (Tom, 2019).

Risk attitudes: It is the way people respond to a given risk situation. Risk attitude affects an organisation's risk appetite. Risk appetite and risk altitudes need to be align in order for the organisation to achieve its objective by taking the right amount of risk. If they are not aligned, a wrong risk threshold will be set leading to high or low information security risk appetite. Risk appetite and risk attitude needs to be aligned else there will not be an appropriate threshold leading to over or under risk intake. Risk attitude can be influence by feelings and past experience and can be modified and change anytime. (Barone, 2019).

Inadequate knowledge of risk appetite: most management do not have sufficient knowledge about risk appetite so they turn to neglect it. Risk appetite becomes a burden to them due to their lack of knowledge. If they try to do it they end up doing it wrongly. A project manager with a good knowledge and many experiences will be confident in making risk appetite decisions thus being able to take more risk (wang et al, 2015).

4 Proposed solution to Risk appetite assessment tool

Risk appetite consideration during decision-making within businesses today lacks the necessary attention it deserves. Most information security professionals turn to guess work during risk assessment, rather than depend on a well-researched and developed risk appetite document. In other to encourage the use of such an important document, this chapter proposes the design and implantation of a simple tool that can be deployed by businesses as a starting point.

4.1 Risk Factors

Risk appetite depends on what an organisation does, what type of data they use, which sector they are in, what legal and regulatory requirement they have to comply to. Below are the different factors which are considered in this proposed solution. It includes the design requirements for developing a comprehensive risk appetite document. The list is not exclusive and the scope will cover both small and medium size organisations.

4.1.1 Business Sector

There are many different business sectors such as government, telecommunication, legal services, construction, food processing, Consultant Company, gambling, retail sales and so on. In most countries, the Government business sectors refers to those businesses own and controlled by the state. Government business sector deals a lot with people's private information and will do everything possible to prevent any breach. Their services are often cheaper or even free thus attracting a lot of customers whose data are recorded in their system. Businesses owned by the government will have a low risk appetite since their primary objective is to meet the growing needs of the people rather than profit maximisation. Government own business risk appetite are also restricted by certain rules/regulations which defined the type and level of risk an employee can take.

Telecommunication business are those types of business that deal with different kinds of communication such as phone and internet. Such business keeps a lot of customer's vital information which if breached will cost the company a lot of money. Their market continue to grow every day with a high demand for their goods and services. Such business sector will have little risk appetite since growth is automatic and fear of loss of customers due to data breach. If a customer's conversation or chat is leaked by hacking, it leads to scandal and loss of reputation to that customer. As a result of that, customers lost trust in that organisation. The customer may sue the organisation and in effect the organisation suffers financial lost. Such businesses therefore will have very little risk appetite for fear of breach and its consequences.

Legal services business sector by nature is risky. Every legal services practitioner have a high risk appetite due to their huge desire for more money. They more successful risk they make the more client they have and the more money they make. They have the advantage of not putting customer's information online thus exposing them to less risk of breach. Breach of information in this case often comes through third parties such as communication media who may publish some sensitive information intentionally or unintentionally.

Construction business sectors have very little information about their client. Their clients are less exposed to information breach but if that happens, the company will be held responsible. They may decide not to put their client's information on the internet thus reducing their chance of data breach. Such business sector will have a high appetite for risk.

Food processing business sector can be liken to construction business sector in terms of risk. When the food processing business sector operate online, more safety measures have to apply to prevent the breach of customer's information. The risk of breach for such business sector is low and this will motivation to have a high risk appetite. When customers order certain food they go ahead to enter their information online. This information could be restricted to basic information about the customer and not their sensitive information such as credit card details. Thus making the breach of information have little or no effect on the customers.

For example customers may be allowed to pay on delivery thus preventing them from entering their credit card details online. If this must happen such as is the case of online shopping, the company need to reduce their risk appetite and ensure more secured protection.

Consultant Company business sector usually have a high risk appetite. They may go online but would not have their clients' sensitive information put online. This therefore reduces their risk of sensitive information breach. The risk of breach is high if they have an online assessment software to allow client access certain areas of their businesses otherwise the risk is low.

Gambling business sector would normally have a high risk appetite. The business by nature is risk taking and the high the risk, the higher the probability to win. Risk taking is not only done by the business owners but also by the client as each party strive for a win and get more money.

Retail sales business sector are business sectors that would sale products directly to consumers. They may have a record of their customer's information online. Most retail shops goes online and faces the risk of having customers detail information in their server. This mostly happen when customers use their credit cards to pay for goods online. This is very risky because such information could be hacked. Most retailers have very little risk appetite in a hope to protect their customers.

4.1.2 Business Type

Different business sectors have varied business types and these business types have different appetite for risk and are exposed to different types of risk. Considering the business sectors above, we are going to discuss the risk appetite for the different business types.

Government business sector deals with many different business types such as banks, schools, and hospitals, insurance and transport agencies. Each of these business types have a different risk appetite depending on their activities. For

instance a hospital has to deals with highly confidential records of their patients. So it is place under strict rules and regulation which may limit their risk appetite. Some government agencies like transport services may be allowed to have a high risk appetite because there is a little risk of data breach.

Telecommunication business sector could be split into telephones companies and internet service provider business types. Both business types deals with customers' data and some have access to customer private communications. Their services are of high demand in the market and they are faced with high risk. These business types have a low risk appetite because they have to handle a lot of sensitive data.

A Legal firm within the " Legal services" business sector may be offering legal services like helping other businesses with their intellectual property (IP) filing, court cases on IP violation by 3rd party, court cases from violation by internal employees, etc. Such a business will be dealing with confidential information from its clients. This information need to be protected. The risk appetite is affected by what services the firm chose to specialise on.

There are many different types of construction companies depending on the job they carryout. Some construction companies include road construction, house construction and railway construction. Road construction possess little risk appetite when compared to house construction. Railway construction is also of less risk appetite

Food processing business sector has to deal with a variety of food stuffs. This sector could be split into perishable, non-perishable business types. Companies with perishable or fragile food stuffs will have a high risk appetite because they want to get their food sole faster and in time to avoid damage and hence loss. They can open up warehouses in area associated with high risk of float if there is a high demand of their goods in such an area. But for a company with non-perishable or non-fragile food will take time to sell its product and will not be interested in high risk appetite.

There are many different types of consulting companies such as IT consultant, business consultant, environmental consultant, software consultant, sale consultant and so on. Over the years, IT consulting company have grown so fast and large. As days goes by, there is an increasing demand of consultant in the different areas of IT. IT consultant will take less risk because a little breach in their business sector will cost the company a lot of money. Business consultant would rather take more risk in order to have high profit. There are different areas of business consulting. Environmental consultant would have high risk appetite because it has very little sensitive data. Software consultant have little risk appetite because the information need to be kept secret. Sale consultant would also have a low risk appetite. This is so because different company's data need to be kept save and well protected from their competitors.

Gambling could be for fun or to generate income. Both have similar high risk appetite. Gambling business types include casinos, Card games, slot machines and so on. Gambling business is by nature a risky business due to the uncertainty of the outcomes. It is risky both on the side of the owner and the gambler. The owner get into higher risk in order to make a higher profit and the gambler also engages into higher risk all with the aim of winning more money.

Retail sales business have different business types such as cloth, groceries, food, books, furniture and so on. Each retail business would have different risk appetite. Food retailer would have a high risk appetite compare to cloth retailer. This is because the food does expires and the industry would like to sale the food out as quickly as possible compared to clothing industry.

4.1.3 Data

Different businesses deals with different data types. Some with just a single type and others with multiple data type. Data could be place in three categories which are confidential, internal and public.

Confidential data: Highly sensitive information intended for specific use. Unauthorised disclosure, modification, or lost would cause significant harm to the interests of the company. Companies with such data will have a low risk appetite. For their protection level**,** explicit authorisation from the management is required for access. All employees handling confidential information are responsible for its safe keeping. They have to respect rules such as; must be provided the highest level of security, must not be transmitted or stored unencrypted, must not be shared without authorisation, and must not be shared over email without encrypting with a key and/or a strong password. Examples of such data include; customer personal information, such as name, telephone number, home address, email, date of birth, username, and password. Employee sensitive information, such as medical records, salary, religious belief, Inc. other HR personal records. Cardholder data, such as PAN, debit/credit card expiration date, CVV and company intellectual properties.

Internal data: Private information that unauthorised disclosure, modification, or lost would be detrimental to the interests of the company. For their Protection level, available on need to know basis. Restricted to employees with legitimate reason to access. Protected due to privacy considerations. Examples of such data includes: Meeting note, business plan, project initiation document, project requirement documents, network diagrams, system design, use case, reports. Employee personal information, such as Employee's Name, Telephone number, Address, Date of birth and contracts.

Public data: Private information that unauthorised disclosure, modification, or lost would cause no damage to the company. Intended to be provided to anyone without restrictions, but may be subjected to appropriate review in other to mitigate risk - disclosure must not expose the company to any financial loss or legal action. Such data will have a high risk appetite. For its Protection level: While subjected to some disclosure rules, information classified as public are available to all employees, including contractors, and entities external to the company. Examples of such data includes; publicly available press release, publicly available marketing material.

4.1.4 Geographical Location.

A company's geographical location refers to the physical location of the company on the earth surface. Geographical location could be, a country site, city, or international. Some companies increases their risk appetite by establishing more companies in different geographical locations. When a company is establish in a country site, a city and abroad, this kind of company is said to have a high risk appetite. A company that remains only at the country site and is reluctant to expand, have a low risk appetite. Companies that are located in areas with high natural disaster have a high risk appetite than those located in a more secured place. Company location could also be continental. That is, located in Asia, America, Europe and so on. Companies located in a continent such as Africa will desire a low risk appetite because of the high level of risk and little or no security. In Europe companies turn to have high risk appetite due to their high level of business security.

Moving data from one location to another is by itself risky. It requires experts to perform this duty to avoid failure. Some data may require the movement of robust physical server. Some devices, when moved may not function anymore. It may require a good planning to move physical hardware with data. Moving data from one location to another is also costly. Some people underestimate the cost and end up in frustration. The cost of moving data may reduce a company's risk appetite. The legal requirement needed to move data from one location to another may not be favourable thus discouraging companies and resulting to low risk appetite. Moving data from one geographical location to another such as across boarders requires that one complies with the legal requirements of the intended new location. Some of these requirements could be so tough and limits the risk appetite of an organisation. For example the data protection Law for EU citizens may prevent US companies from moving data from EU to US. Some legal requirement may not support the migration of data from certain countries. There are some data that cannot be migrated for some specific reasons. Some issues that may occur during the migration may require legal backup. So one has to ensure that every step made are legally back up.

4.1.5 Company size

The size of a company is not determined by the size of the building but by the headcount and/or turnover. Same types of risk face companies with similar activities irrespective of the size. Companies with varied activities and faced with different types of risks. A company with a large number of employees have a low risk appetite when compared to a company with small number of employees. This is because, with more employees, the more the variation in risk culture and may slow down risk decision. But with a smaller number of employees, the risk decision is faster and swifter. Employee education on risk appetite could also affect the risk appetite. A good knowledge of risk appetite by employee may increase their appetite for risk and vice versa. Also, a company with large turnover would also have a high risk appetite since they have sufficient income to treat their risks.

4.1.6 Business Objective / Security Objectives

Different businesses have different objectives such as survival of first year, just to make profit while others like NGOs or public companies have as objective to serve the public effectively in a particular dimension. Making Profit Company will turn to make a lot of risky decisions especially if it'll allow them to make good profit – and these decisions might need the board to accept the risk. The business objective of a company will determine its level of risk appetite. Companies that are aim at just surviving the first year will have a low risk appetite while those that are aim at making high profit will have a high risk appetite. The security objectives of a company most align with the business objectives. There are many security objectives. The security objective of a company must be chosen in a way as to help achieve the business objective thus guiding the amount and type of risk the company will be willing to take. The business/security objectives of a company changes over time thus leading to a changing risk appetite.

4.1.7 Legal and regulatory Requirements

The legal and regulatory requirements of a business could be established from loss cost by threats and vulnerabilities or between trading partners, contractors, services providers, organisation, or designed and developed by organisation to help manage its information system. Legal and regulatory requirements are expected to be compile to by organisations. Such requirements could fall under national security, corporate governances, electronic commerce, identity theft/data protection, and intellectual property protection. Legal and regulatory requirements are set by an authorised body and are enforced through sanctions. Each country or continent has a well establish legal/regulatory requirement which they have to comply to. For example all European business organisation and businesses out of European Union dealing with data of European citizens have to comply with GDPR regulatory requirements for privacy/data protection. When the legal and regulatory requirement has a high sanction, the organisation will desire a low risk appetite. Some legal and regulatory requirements intentionally limits the risk appetite of a company while others require the company to present a risk appetite statement.

4.1.8 Security Threat Level

Information security threat level is determine by performing penetration testing using a vulnerability scanner. By so doing, they amount and types of threats are determined and the company would be able to determine their level of risk exposure. The more the vulnerability, the higher the threat level. At times, something can be done to reduce the level of vulnerability otherwise it is a big risk factor to the company. Understanding the vulnerability and threat level will influence the organisation’s risk appetite. If the level of vulnerabilities high, obviously the threat level will be high, thus the organisation might be tempted to take little risk leading to a low risk appetite. On the other hand if the threat level is low, the organisation will take more risk thus portraying a high risk appetite.

4.1.9 Stake Holder Interest

In an organisation, there are different groups of stakeholders with different interest, background and different point of view. Normally, the board of directors are often in charge of setting the risk appetite of an organisation. They do it according to their experience, personality and knowledge. A director with high experience and good knowledge of risk appetite will likely have a high level of risk appetite while an inexperience director will have a low risk appetite. Risk appetite differ between business units. If a director has worked in a business unit with high risk appetite, he would most likely to take more risk and vice versa.

4.1.10 History of Data Breach

Organisation who have a high record of data breach recorded in their achieve, would have low risk appetite. This is due to their bad experience and they would not like the situation to occur again hence they would be more careful. While those with a low record of data breach would have a high risk appetite because they have the feeling that they are save.

4.2 Risk Appetite Guide Lines

There are some other things which a company need to establish as a guide line to their risk appetite which shall be considered in the design of this algorithm. These factors are to be provided by the company and it will be compared against the calculated risk value. This include the following: Strategic objectives, Risk appetite statement, Risk threshold

4.2.1 The strategic objectives of information security in business.

Strategic objectives helps in the establishment of a good risk appetite statement. Every business sets strategic goals and objectives in order to enable careful business monitoring. The strategic objective of information security in business

is centred on three basic areas. These areas are availability, integrity and confidentiality. Any breach in any of these three areas, could lead to financial lost, reputational damage and loss of customers. Confidentiality ensure that information is accessed only by the right person. Those who are not allowed to have access to the information must be prevented. Confidential information are those that are not to be granted access to by any type of person but only for particular people. Those having access to such information must understand the risk associated to its exposure and how to prevent such exposure. Integrity ensures that the information is not tampered with. Some people may attempt to alter data especially when the data is in transit. Checksums is one of the most common ways to verify data integrity. Availability ensure that data are always available for use by users. Any business that will not ensure availability to the users will lost trust from user and this may lead to loss of customer and thus drop in profit.

4.2.2 Information security Risk appetite statement(s)

The business objectives of the company guides the risk appetite statement(s). The risk appetite statement(s) is a standard documents which determine how the company will function in the area of risk taking. It establishes risk boundaries for return on profit. Risk appetite statement(s) should be developed in collaboration with the board members and valuable stakeholders. The risk categories are identified (breach in availability, confidentiality and integrity) and risk statement is made for each of them. The risk appetite statement(s) has to be communicated to all stakeholder within the organisation.

4.2.3 Determination of information security risk threshold.

Organisations should be able to tell the amount of risk it is willing to take in monetary term. The amount of risk should have a match with the amount of money it is willing to loss if such incident occurs and the business still survive. This could be presented in percentage of a given working capital. Risk appetite

should fall within the company's risk threshold.

4.3 The Model

There exist different types of algorithms for various purposes and these algorithms have different requirements. In our risk appetite algorithm, the requirements include: the design, flow diagram. Factors consider above, companies risk threshold and risk appetite statement.

4.3.2 The Design

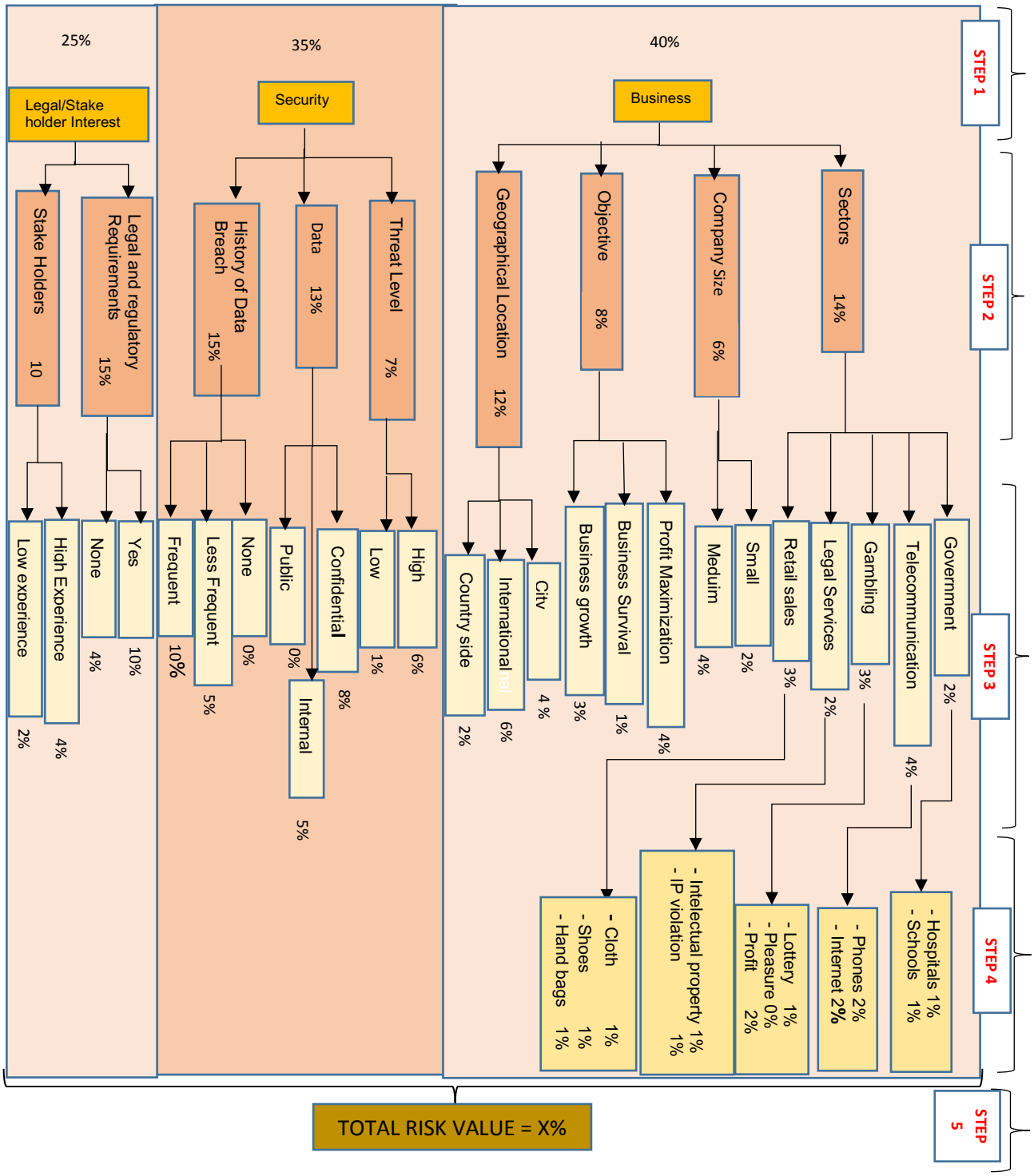

Fig 2. Risk Appetite Design

Step 1: The above risk appetite diagram illustrate the design of factors affecting risk appetite. At step 1, we have the roots also known as level 1. This level include; Business, security, legal/stake holder interest. These are factors that influences the risk appetite of a company. They are then separated to different branches. The amount of risk for these factors is given in percentage of the total risk value. The sum of the risk value here in percentage is 100%.

Step 2: The brown boxes are the stem also known as level 2. As we advance, each level sum up to the total of the previous level. For example the total for the security is 35% which is shared into Threat level, Data and History of Data breach. Here we have; Business = 40%, Security = 40% and legal/stakeholders interest is 20%. At the level of security, the threat level has the smallest percentage of 7% because when compared to the other factors like data and history of data breach it is less risky. Threat level could easily be minimised using different prevention methods. When a company has a frequent history of data breach, it is more risky because to take high risk. If a company has a high threat level, the risk value is 6% but if the company has a low threat level, the risk value is 1%.

Step 3: While the pale-white boxes are the braches also known as level 3. They also sum up to the previous risk value of each factor.

Step 4: Here we have the risk value for different departments in a company. This risk values for different areas in a company might be different depending of their activities.

Step 5: After analysing the risks and their values for a company, the risk values are then summed up to give a Total Risk Value. This total risk value is then compared with the risk appetite statement(s).

4.3.3 The Algorithm

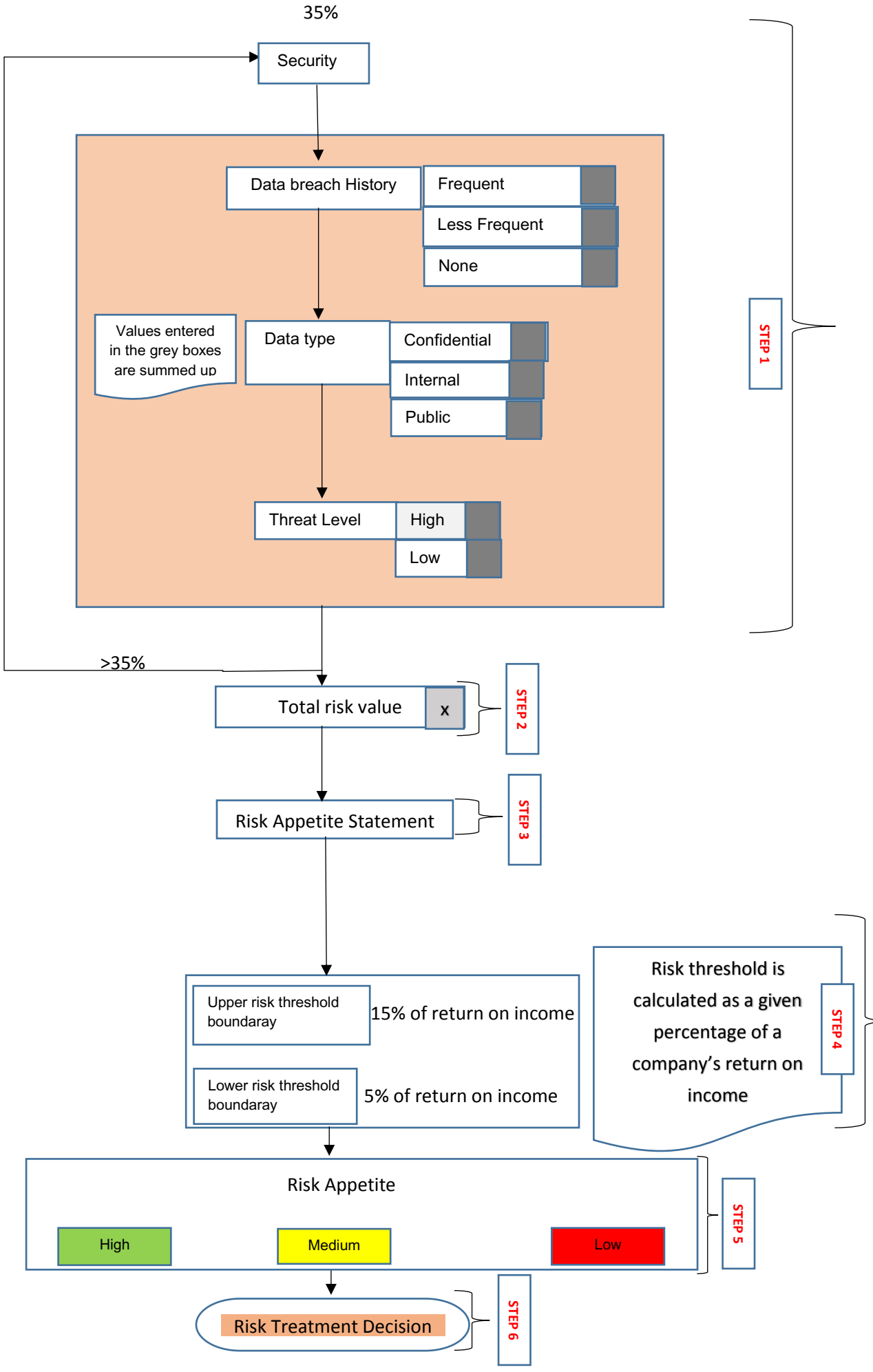

Fig 3. Risk Appetite Algorithm

Step 1: For the purpose of clarity and in order to avoid an overcrowded diagram, one section of the design (Security) is chosen and elaborated on. Security could be divided into 3 different areas. These areas are further broken down to sub areas. Companies need to choose which areas relates to them and their given values registered automatically by the machine. These values are then summed up to give total risk value.

Step2: The Total Risk Value is calculated by summing up all the risks associated with the different factors as shown in figure 3 above. Total Risk Value must not be greater than 35% else the process need to be repeated.

Step 3: This Total Risk Value is compared against the Risk Appetite Statement(s) of the organisation. This statement(s) specify the type of risk and what quantity the company is willing to handle.

Step 4: The algorithm then check that in the risk appetite statement(s), the considerable risk should fall between the upper and the lower limits of the risk threshold. The value of risk threshold is determined by the company depending on how much they are willing to spend on a given risk type.

Step 5: When we get the risk appetite value, we then check if it is low, medium or high. The risk appetite statement will help us determine this.

Step 6: Knowing whether the risk appetite is low, medium or high, enable one to determine what kind of treatment is good for each risk.

4.3.4 Sample illustration of the Algorithm

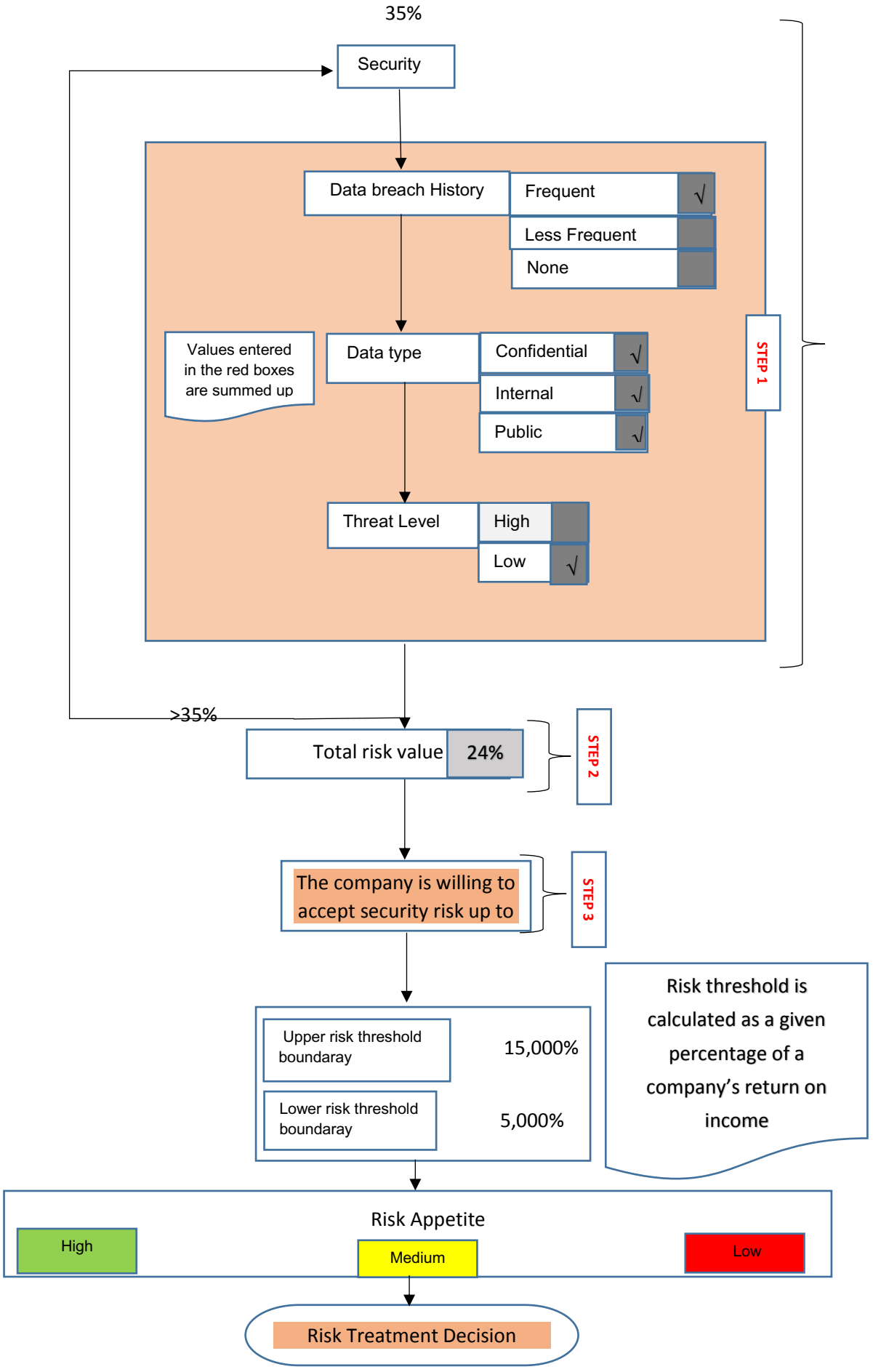

Fig 4. Sample illustration of the Algorithm

Considering a small size company whose working capital is $100,000. Its upper risk threshold limit is $15,000 (15% of the working capital) and the lower risk threshold amount is $5,000 (5% of the working capital). From the design in fig 2, the maximum risk percentage for security is 35% which is broken down into the different risk areas (Data breach history, Data type, Threat level). Data breach History is Frequent so, the value is = 10%. Data type for the company are Confidential, Internal, and Public thus the value is = 13%. Threat level is low so the value =1%. Total risk value here = 24%. If the total risk value is greater than 35% for this area, it implies there was an error somewhere and the process needs to be repeated again. This company in her risk appetite statement, is willing to spend $10,000 in security risk. This decision and statement is made by the company (Board of directors and chief information officers in some companies).

If the company does not prevent the risk of Data breach, Data type and Threats, any breach of these three areas will cost the company 24% of $100,000 which is $24,000. So the company will rather spend $10,000 to guard against such breach rather than losing $24,000. If the total risk value is > 15% of working capital, the company will have a low risk appetite, if it is between 10% - 15% of the working capital, the company will have a medium risk appetite but if it is <10%, the company will have a high risk appetite. Below is a sample risk appetite for statement for the illustrated case.

4.3.5 Risk appetite decision table for Security level

Not more than 4,000$ should be spend to reduce the threat level as low as possible. Not more that 6,000$ should be spend on data breach or not more that 4 out of 10 customer should complain about data breach.

IMPACT	Percentage	Effect	Decision	Treatment decision
High	>=15% or > 6 customer out of 10 complain	Cost the company about 15,000$ or more	High risk affects the risk appetite negatively.	
Moderate	10% to 15% or 4 to 6 customer out of 10 complain	Cost the company about 6,000$ or less	Moderate risk lead to moderate risk appetite	
Low	<=10% or <= 2 out of 10 customer complained	Cost the company about 5,000$ or less	Low risk lead to high risk appetite	

Table 4. Risk Appetite Decision Table for Security Level.

When the risk is high, the risk appetite is often low. When the risk is moderate, the risk appetite could also be moderate and when the risk is low, the risk appetite is high thus risk is inversely proportional to risk appetite. With this knowledge, the company will be able to make best treatment decision to either accept, share, transfer or reject the risk. This decision varies from companies to companies that is why no treatment decision is made in table 4.

4.3.6 Assumptions Made In developing this algorithm

The first assumption is that, this algorithm is used only for data security of medium and small size organisation. Also for simplicity purposes, development is done on one general factor (Security) that affect risk appetite. Again, questionnaire is develop for all factors (Security, business, legal/stakeholder interest) and distributed to companies using a given link.

5 Case Study: Local business

In this thesis, small and medium size business were taken into consideration. A questionnaire was designed using Survey Monkey (https://www.surveymonkey.com). It had 10 major questions with sub questions. A link (https://fi.surveymonkey.com/r/2CM2MPP) to the questionnaire was distributed to different small business companies which were randomly chosen. When I got the replies, I did a close examination and the result where entered into the table below. Responds were obtained from five companies. These companies could be put under these sectors: Retail Sales1, Logistics, Medical care, Construction, and Retail sails 2. Each factors and the risk associated to that factor in relation to the company is recorded in table 5. One of these companies (Retail Sales 2) is chosen as the case study and analysed in detail bellow.

Sector	Risk due to the business sector	Business Type	Risk due to the business type	Company Size	Risk due to the company size	Objectives	Risk due to objectives	Geographical Location	Risk due to Geographical location	threat levle	Risk due to threat levle	Data type	Risk due to Data ttyoe	History of Data braach	Risk due to History of data breach	Legak/regulatory requirements	Risk due to Legal/regulatory requirement	Stake holdrers	Risk due to Stake holder interest
Retaial sale 1	3	Furniture	2	small	2	Meet customer's expections	3	contry side city	6	low	1	internal Public	5	None	0	Yes eg. GDPR	10	Low Experience	2
Logistic	4	Logistics	4	medium	4	Customer's satisfaction	3	City international	10	high	6	confidential internal public	13	None	0	Yes eg. GDPR	10	High Experience	4
Medical care	2	Home care for ederly	2	small	2	Customer satisfacton business growth	3	country side city	6	low	1	confidential internal public	13	None	0	Yes eg. GDPR	10	Low Experience	2
Consturcit on	3	Floor maintainance	2	small	2	Business surviver	1	City	4	low	1	internal public	5	None	0	Yes eg. GDPR	10	High Experience	4
Retail sails 2	3	Groseries	3	medium	4	Profit Maximisation	4	Country side city international	12	high	6	confidential internal public	13	None	0	Yes eg. GDPR	10	Low Experience	2

Table 5: Result From Questionnaire

Companies risk can be rated due to their sector. Logistic has a high risk value of 4 due to the nature of the business. Most often, all information about its management are put online and it is shared with those in other locations. Information such as goods type, customer's details and lot of confidential information about transaction are registered online and if a hacker breach into the system, he will definitely get a lot of information to influence.

When the size of the company is large, there will be high financial loss if data breach occurs. Large companies would also have to deal with a large number of customer's data and more employees which makes data security control a bit difficult and costly. It is more difficult to train the employees to manage data effective. For instance in 2019, Facebook was breach due to poor security and this affected the data of about 540million people.

When they company has an objective to maximise income, it would do everything it can to have a high desire for risk. Just like the saying goes "more risk more reward and No risk no reward". They would not mind investing even in areas of natural disaster.

As companies grow and expands to more location including abroad, so too does their risk value increase. A company that is not willing to take more risk, is not interested in growth and would prefer to remain local. Threat level also influences risk. Logistic and Retail Sales2 have a high level of threat which makes it more risky for hackers.

When the stake holders are more experienced, they are ready to take more risk unlike and inexperienced stake holders who are afraid. Legal and regulatory requirement is high because it is mandatory and comes with a fine if failure to observe it happens. Worse of all, if client have a legal claim over a company.

5.2 Implementation and Testing

Company chosen for implementation and testing is the Retail Sale 2. This is a groceries retail company and it is associated with more risk when compared to the other listed on table 5 above. It is a medium size company and have a risk of 4% due to the company size. Its objective is to maximize profit so the company is ready to do anything to achieve its gaols such as, taking more risky activities. They are located in country site, city and abroad. These makes their risk due to geographical location to be 12 and they have a high treat level with a value of 6. They handle all classes of data (Confidential, Internal and Public) which make their risk value in this area be 13. They have no history of data breach and they are restricted by legal/regulatory requirement. Stake holders here have a high experience and so their risk due to stake holders' interest is high. So the Total Risk Value is 57%. The companies Return on income is $120,000

Considering just the security level, the maximum risk should be 35%. In our case study we have the value of 19% or $22,800 which falls below 35% thus is accepted. The value of 19% indicates that, the company have a medium risk appetite. But now the company is willing to spend no more than $18,000 for all risk that concern security. In this case it is better for the company to treat this risk by transferring it to third party at a moderate cost. Fig 5 and table 6 illustrates this.

Retail Sales 2

Impact	Possible Negetive Situation	Quantity of Data invovled	Possible loss if situation occurs	Response time	Treatment Decision
High	□ loss of key customers. □ Multiple customers take on legal actions. □ Regulatory enforcement action/ fines □ loss of consumer trust in one or more of our brands	>100,000	>= 20% loss in income Or >= 24,000	3hrs - 3days	
medium	□ Target for hacktivists □ Social media storm	10,000 - 100,000	5% - 20% loss in income Or $6,000 - $24,000	1day-7days	
Low	□ Colleague employment dispute /action □ Stake holder less interested in security □ Unhappy customer/Complaints □ single customer dispute/legal action	<10,000	<= 5% loss in income Or <= $6,000	1day to 2 weeks	

Table 6. Risk Appetite Decision Table for Retail Sale.

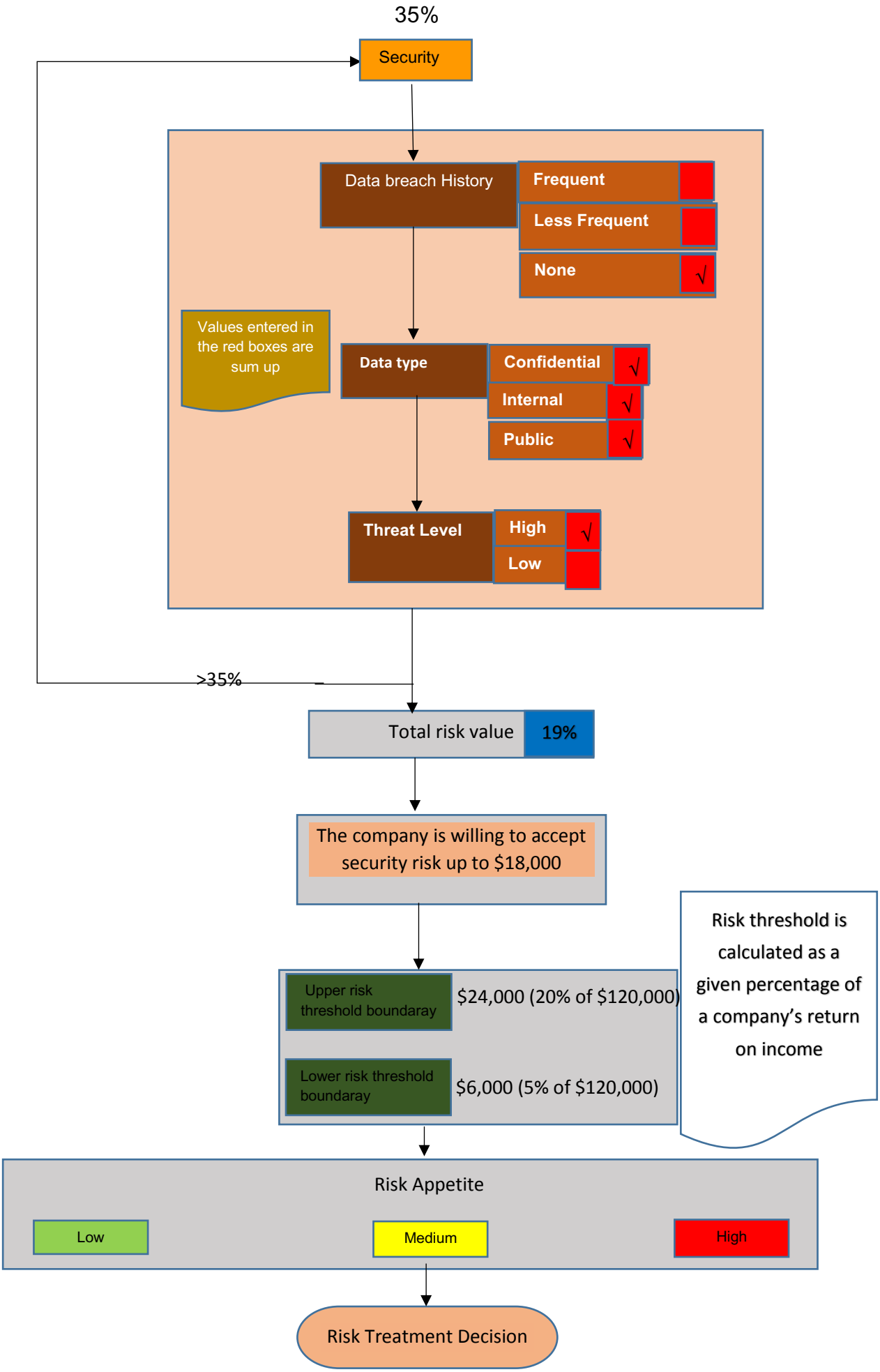

Fig 5: Case Study Risk Appetite Algorithm Analysis

6 Using Machine Learning Algorithm to check Risk Appetite.

Machine learning is a data analysis method that is used to automate analytical model building. A machine learning algorithm learns from a data, identify patterns and make decisions with little human intervention. Two types of machine learning algorithm are Supervised and Unsupervised machine learning algorithm.

A supervised machine learning algorithm deals with labelled data. It learns from the training data and predict the output based on the training data. Common algorithms in supervised learning include linear regression, logistic regression, naïve bayes, support vector machines, artificial neural networks, and random forest. These algorithms are peculiar to different types of data. For example, if the data used for the analysis is a continuous value such as predicting the salary of workers, a linear regression machine learning algorithm can be used in predicting the salary of the workers and if the data have a lot of classification and difficult to separate, a support vector machine learning algorithm can be used to predict the desired output (Davin, 2018).

Unsupervised machine learning mostly perform clustering, representation learning and density estimation tasks. Exploratory analysis and dimensionality reduction are two types of unsupervised learning. Exploratory analysis enables the structure of the data to be identified while dimensionality reduction unsupervised machine learning enables large set of data to be represented using less columns or feature (Davin, 2018).

6.1 Project Implementation with Python

The goal of every manager is to minimize the company's risk in order to increase the company's risk appetite thereby enabling the company to engage in more projects that will promote their growth. This can be easily achieved with machine learning, where a model is created and trained to determine the risk appetite of the company based on the company's labelled data, when there is a need to

update any factor influencing the sector's risk, this model can be used to predict the company's risk appetite, which will serve as a guide on the decision making in order to maximize the risk appetite.

Given the risk appetite factors in this local businesses and their sample risk values, the total risk values can be calculated and used to determine the risk appetite of the company. If the total risk value of that sector is more than 0.40 (40%) for example, the company might not be willing to engage in the projects thus their risk appetite is low (denoted as 0). Whereas if the total risk value of the business is less than 0.40 (40%), the company will be willing to engage to projects that could lead to their growth, thus a high-risk appetite (denoted as 1). As shown in table 7.

Business	Sector Risk	Sector Risk	Objective Risk	Geographical Risk	Treat Level Risk	Data Type Risk	Regulatory Requirement Risk	Stake Holder Risk	Total Risk	Risk Appetite
Retail Sales 1	0.03	0.02	0.03	0.06	0.01	0.1	0.1	0.02	0.37	1
Logistic	0.04	0.02	0.03	0.1	0.06	0.13	0.1	0.04	0.52	0
Medical Care	0.02	0.02	0.03	0.06	0.01	0.13	0.1	0.02	0.39	1
Construction	0.03	0.02	0.01	0.04	0.01	0.1	0.1	0.04	0.35	1
Retail Sale 2	0.03	0.03	0.04	0.12	0.06	0.13	0.1	0.02	0.53	0

Table 7. Risk per Factors in Percentage.

Using the risk appetite factors from the local businesses, a data set consisting of the following variables was created.

Firstly, sector: These are the different sectors operating in the company. They include the following Logistics, Medical Care, Retail Sales1, Retail Sales2 and Construction. Secondly, sector risk: This is the risk value involve in each sector. Thirdly, type: This is the type of services that are provided in each sector, they include Logistic, homecare, Groceries, Furniture, Floor maintenance. Fourthly, Type Risk: This is the risk value due to the service type. Fifthly, objective: The main objective of the sectors could be Profit Maximization, Customer Satisfaction, Meeting Customer Expectation or Business Survivor. Sixth, objective risk: This is the risk value due to the sector's objective. Seven, geographical location: This is the location where the sector is operating. The sector can operate in the Country Site, City or City, International. Eight, geographical location risk: This is the risk value due to the sector's location. Nine, treat level: This is the level of treat that the company have experienced. It can either be high or low. Ten, treat level risk: This is the risk value due to the treat level. Eleven, data type: The data used by the sector are either Confidential, Internal & Public or that at both Internal &Public. Twelve, data type risk: This is the risk value due to the data type. Thirteen, regulatory requirement: This is the legal influence on the business. Fourteen, regulatory requirement risk: This is the risk due to the influence of the legal regulatory on the sector. Fifteen, stake holder: The level of experience that a stake holder has. The experience level could be low or high. Sixteen, state holder risk: This is the risk value due to the state holder experience. Seventeen, total risk: This is the summation of the factor's risk values (type risk values, objective risk values, geographical location risk values, treat level risk values, data type risk values, regulatory requirement risk values and the state holder risk values). When the total risk is less than 0.40(40%), then the sector is defined to have a Low-risk which could lead to high-risk appetite and if the total risk is greater than 0.40(40%), the sector will have a low-risk which could lead to a low-risk appetite. Risk Appetite; This is how much risk a business is willing to accept or reject based on a total risk value. If many factors have a high-risk appetite (that is low Risk

Value), then the company in turn will have a high-risk appetite and it will be open to growth.

6.1.1 Data Visualization

A visualization of total risk value by the risk appetite factors is shown below.

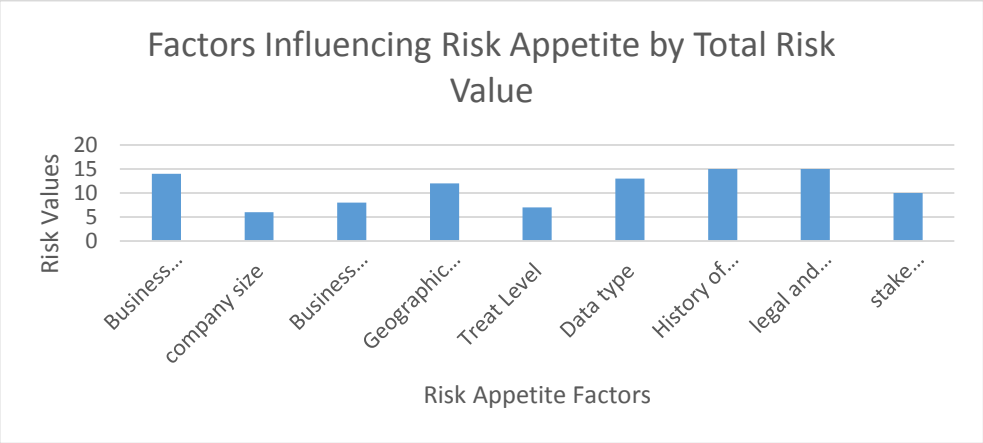

Fig 6. Factors Influencing Risk Appetite by Risk Value.

Risk appetite factors such as history of data breach and the legal and regulatory have the highest risk value while that due to the Company size has the least risk value (Figure 6). Factors with higher risk value result to low risk appetite while those with a lower risk value result to high-risk appetite. Therefore, history of data breached as well as the present of legal and regulatory in this business greatly influence its risk appetite.

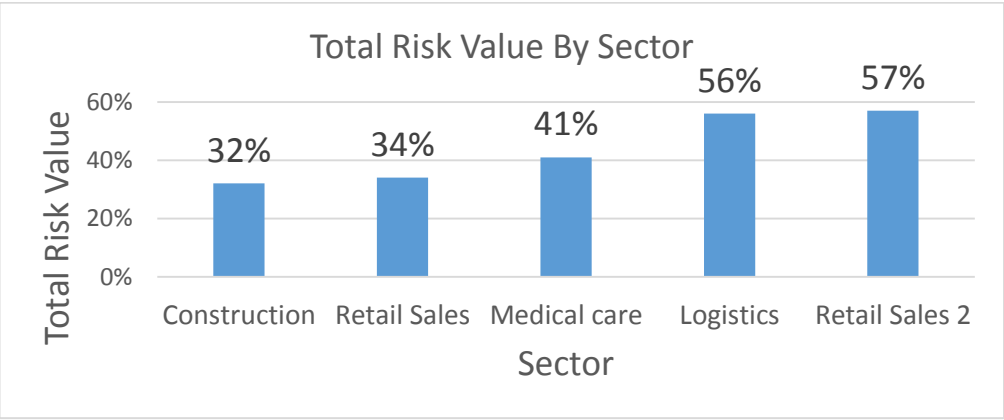

Fig 7. Total Risk by Sector

Two companies use the sector Retail Sales. Retail Sales1 deals with furniture while Retail Sales2 deals with Groceries. Retail Sales2 recorded the highest risk while the construction sector recorded the smallest risk value (Figure 7). Therefore, the sector that deals with grocery will have a high-risk value which implies that its risk appetite will be low. The Construction sector on the other hand will be willing to accept new projects since it has a low risk value implying that their risk appetite is high.

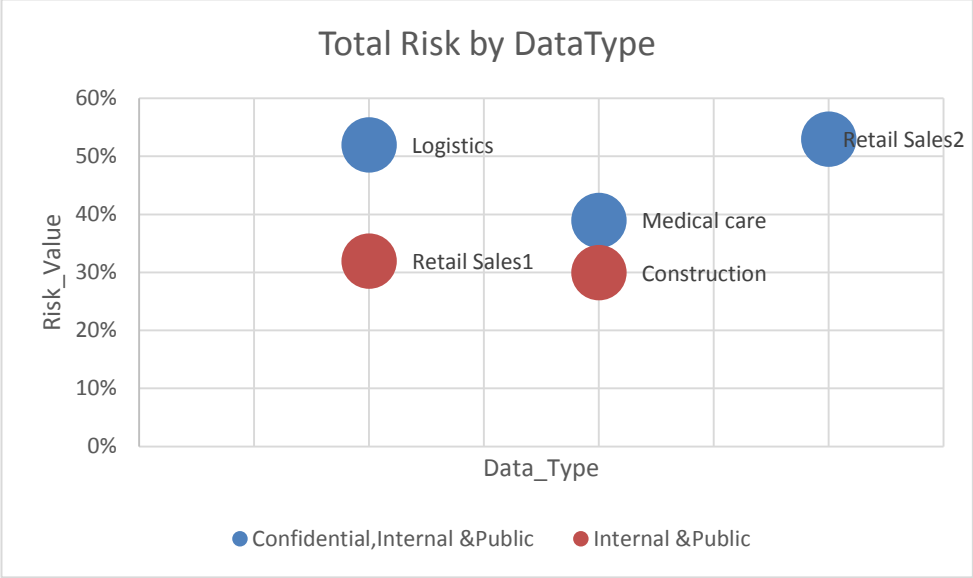

Fig 8. Total Risk by Data Type

The Data type made of Confidential, internal and public had a higher risk value compared to that consisting of only Internal & Public data type with lower risk value (Figure 8). This means when the company data is highly confidential, the company will not be willing take more projects thereby reducing its risk appetite. The data that is not confidential is not exposed to more risks and thus new projects might likely be accepted with such data since their risk appetite is high.

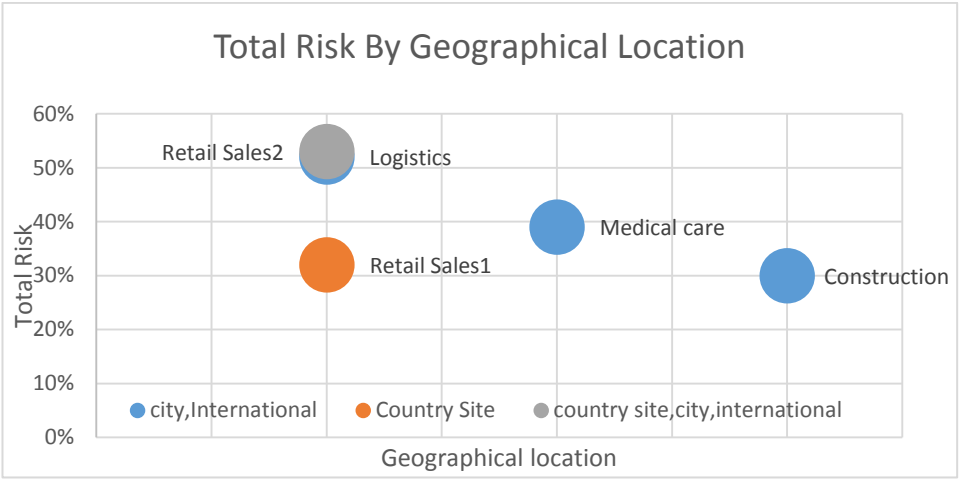

Fig 9. Total Risk by Geographical Location.

Sectors that operated in both city, country and international (abroad) had highest risk values while the sector that operated only in the city and international had the lowest risk value. Therefore, the sectors operating in all regions have low risk appetite and might not be willing to engage in a new project while the sector operating only in the city and international have high risk appetite and can openly accept new project.

From the above analysis, Retail Sales2 sector had the highest risk value properly because they use a large quantity of confidential data and operate in all regions. Thus, they have a low risk appetite. The Construction sector on the other hand had the lowest risk value implying that they might likely accept new changes in their operation thus having a high-risk appetite.

6.1.3 Data Pre-processing

From the visualizations, the dataset has a lot of categorical variables, these variables need to be converted to numbers (decimal) for the machine learning to understand them. This is done in data pre-processing stage. The data pre-processing stage involves the preparation of data for the analysis by dividing data into attributes and labels as well as dividing data into training and testing sets. In this analysis, the following data pre-processing methods were used. Firstly, all the labels of the factors affecting the risk appetites were dropped from the dataset and their risk values were taken into consideration. Secondly, the risk appetite

column was converted to binary (0 =low, 1 =high). The risk values in percentages were converted to float and finally, the dataset was divided to the input and output. The input values consisted of two variables at a time (Total Risk Value and Sector Risk Value) and (Total Risk Value and Geographical Location Risk Value). The output was always the risk appetite. This led to the creation of two types of models which can be used when updating the company's sector's risk value or geographical location risk value in order to maximize the risk appetite.

6.1.4 Training the Machine Learning Algorithm

The support vector classifier from the support vector machine was used to train the model. It learned from the input and output combination and trained a model that can be used in predicting the risk appetite of the company.

Summary of the Training Model

```
SVC (C=1000, cache_size=600, class_weight=None, coef0=0.0,
  decision_function_shape='ovr', degree=3, gamma=1e-08, kernel='linear',
  max_iter=-1, probability=False, random_state=None, shrinking=True,
  tol=1e-10, verbose=False)
```

Fig 10. Summary of the Training Model

This is the summary of the support vector classifier that was used in training the models. The most important parameters that determine the success of the models include; firstly, 'C' (Cost), this is a penalization parameter which control the influence of the support vector and help in reducing error in the models. Higher cost (1000) was used in these models because the data size was small. Secondly, the gamma value (measures the similarity between two points). The gamma value for the models were very small (1e-08) implying that every point was taken in to consideration. Lastly, the kernel function used in building the models. The linear kernel is used in these models because only two set of inputs and 1 output is used in training the algorithm.

6.1.5 Model Testing

Support Vector Machine learning algorithm learned from these two datasets and trained two models that was used to predict the risk appetite of the company. Using the risk appetite factors (sector and geographical location risk values) and the total risk value of the company's sector, a linear support vector machine found a boundary that separated the high-risk appetite from the low risk appetite.

Model 1

Used for predicting the risk appetite of the company as the result of updates or changes in the sector's risk. For instance, given the total risk value of 0.32 and a sector's risk value of 0.03, the actual risk appetite was 1(high). When the trained model is used to predict this risk appetite, the result is 1 as expected. The boundary that separate the high-risk appetite from the low risk appetite based on the total risk value and the sector's risk value is shown in the figure 11 below.

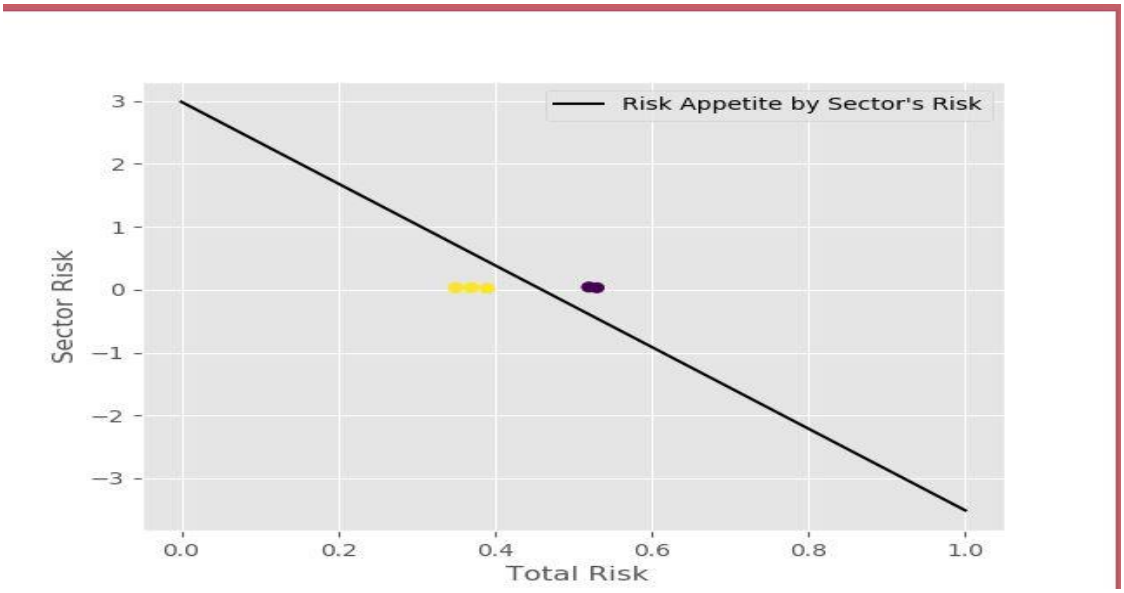

Fig 11. Decision Boundary Based on Total Risk and the Sector's Risk

The straight margin shows the risk appetite decision boundary used by the classifier. From the five data values, the support vector classifier correctly created

that three sectors had a high-risk appetite while two sectors had a low risk appetite. Thus, the model is accurate.

Model 2

Used for predicting the risk appetite of the company as the result of updates or changes in the Geographical Location. For instance, given the total risk value of 0.52 and a geographical location risk value of 0.01, the actual risk appetite was 0 (low). When the trained model is used to predict this risk appetite, the result is 0 as expected. The boundary that separate the high-risk appetite from the low risk appetite based on the total risk value and the geographical location risk value is shown in fig 12 below.

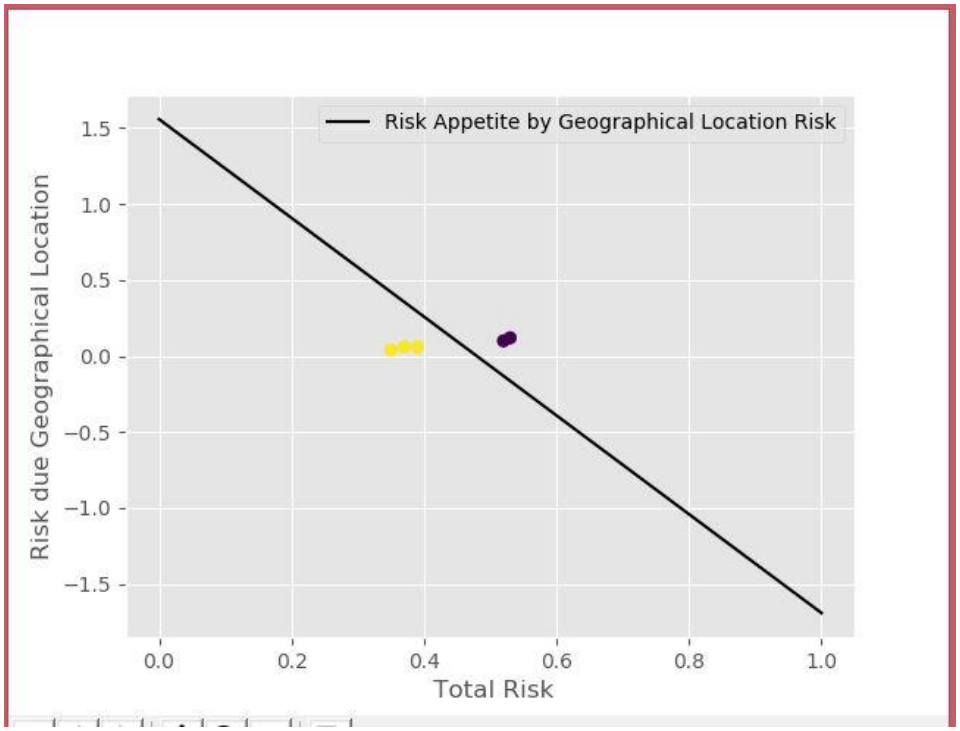

Fig 12. Decision Boundary Based On Total Risk and the Geographical Location Risk

Just like figure 10, the straight margin determines the decision boundary, and the 3 yellow dots indicates the high-risk appetite while the 2 purple dots indicate the low risk appetite. Therefore, model 2 accurately classified the risk appetite.

6.1.6 Making Prediction

After the model is trained, it can be deployed and used for future predictions of the company's risk appetite. For example, if the company want to update its retail sales sector to all groceries but still want to maintain the low risk appetite, the sector can input the suggested risk value that they are willing to take and check whether the risk appetite is low if, not they will adjust the risk appetite accordingly.

To test the accuracy of the models, the prediction function was used to predict the output of all the models. For example, when the total risk value was 0.54 and the sector risk value was 0.03, model 1 predicted the risk appetite to be 0 (Low). This confirms the fact that all the total risk value greater than 0.40 had a low risk value, thus the model1 is accurate. When the total risk value was 0.32 and the geographical location was 0.03, model 2 predicted the risk appetite to be 1(high) thus confirming the total risk value lower than 0.40 had high-risk appetite. Therefore model 2 is accurate.

Therefore, if the company is able to specify the total risk value that they can take in each sector with the risk value that they can take on the risk appetite factors, a dataset can be generated that will train a machine learning algorithm to build models that can predict the risk appetite of the sectors. Thereby, determining the risk appetite of the company. It is recommended that high cost and low gamma support vector machine parameter values should be used to improve the accuracy of the model. If the company want to update some risk appetite factors (for example sector and the geographical) while maintaining the same risk appetite, these models can be used to predict the future risk appetite thereby guiding in the decision making.

6.2 Limitation of the trained Model

Despite the ability of this trained SVM model to predict the risk appetite of the company, it faces the following limitations. Firstly, the data set used in this model is very small which might lead to a significant difference between the Observed value and the predicted value. Secondly, this model has an overfitting effect since

there is a significant difference between the training and the test sets. In addition, this support vector machine learning model will not perform well if the number of features of each data point exceeds the number of training data sample. Finally, it is not easy to choose a kernel function for SVM model. (Maheswari, 2019)

For this model to be considered perfect, the following practices will need to be implemented. First and foremost, the company will need to develop some strategy to collect the company's data on the different risk values taken for every service or process. Secondly, the quality of data inputted in the database needs to be accessed to make sure that the prediction is accurate (Alexandre, 2019). Furthermore, high cost parameter should be used to tune the training data in order to improve the accuracy of the model and finally, the kernel function should be tunned to various types when different datasets are used. This will enable accuracy in training the model (datacamp).

7 Conclusion

This thesis was aimed at addressing the deficiency involved in risk assessment process through the development of a risk appetite algorithm. Assessing an organisations' risk appetite, helps the organisation to make effective risk treatment decision. Risk appetite is the organisations' desire for risk. It is an internal drive which requires one to take more or less risk. This desire could come from within or be a regulatory requirement. An organisation may have same situation with different objective thus different risk appetite. In some cases, an organisation may have high risk appetite but cannot take it because of their inability to handle the. On the other hand, an organisation may have low risk appetite when it has the ability to handle risk. Such organisation need to take the risk in order to fit into the competitive market.

Information security risk appetite is not fixed and need to be reviewed because situations are not fixed. With the use of machine learning, an organisation can follow up their changes in risk appetite. They can also check how each factor causes a change in their risk appetite by increasing or decreasing their risk values. Without an appropriate risk appetite analysis tool there is a sure possibility of organisations doing over security in areas that need little security protection or under security in area that need more security protection.

The reason why most companies do not consider risk appetite in their risk management process, is due to lack of knowledge about it. They need adequate knowledge to be able to consider risk appetite. This proposed solution works perfectly and give a clear guild line and knowledge to those who intern to consider risk appetite in their risk management process. With this sample risk appetite assessment tool, businesses will be apple to appreciate risk appetite and implement it appropriately. Risk appetite does not eliminate risk residual. Risk residual will always be there but the effect can be reduce to an acceptable level.

References

Alexandr, G. (2019). 5 Ways to Deal with the Lack of Data in Machine Learning. (n.d.). Retrieved from https://www.kdnuggets.com/2019/06/5-ways-lack-data-machine-learning.html.

Brett D.McKamey(2018). Understanding Your Risk Capacity - goelzerinc.com. Retrieved from https://goelzerinc.com/uploads/InvestmentCommentaryQtr2.2018.pdf

Barone, A. (2019, April 14). What You Should Know About Risk Profiles. Retrieved from https://www.investopedia.com/terms/r/risk-profile.asp

Calder, A., & Watkins, S. G. (2010). *Information security risk management for ISO27001/ISO27002*. Cambridgeshire: IT Governance Pub.

Chapman, R. J. (2013). Simple tools and techniques for enterprise risk management. Chichester, England: Wiley.

Devin Soni. (2019, July 16). Supervised vs. Unsupervised Learning. Retrieved from https://towardsdatascience.com/supervised-vs-unsupervised-learning-14f68e32ea8d

Erm. (2009, April 15). Risk Culture of Companies. Retrieved from https://erm.ncsu.edu/library/article/risk-culture-companies/

Edgerton, M. (2013). A Practitioners Guide to Effective Maritime and Port Security. doi:10.1002/9781118633151.

Exploring Risk Appetite and Risk Tolerance - RIMS. (2009). Retrieved from https://www.rims.org/resources/ERM/Documents/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf.

Freund, J. (2015). Measuring and managing information risk: A FAIR approach. Amsterdam: Butterworth-Heinemann

Fraser, J. R., Simkins, B. J., & Narvaez, K. (2015). *Implementing Enterprise Risk Management: Case Studies and Best Practices*. Hoboken, NJ: John Wiley & Sons.

Gibson, D. (2015). *Managing risk in information systems*. Sudbury: Jones & Bartlett Learning.

Gravelle L. (2018)Talent Development's Guide to Risk Assessment : ISBN156286783 American Society for Training and Development.

Hillson, D. (2015). Weight loss for risky projects. Newtown Square, PA: Project Management Institute

Hillson, D., & Murray-Webster, R. (2007). *Understanding and managing risk attitude*. Aldershot, England: Gower.

Hopkin, P. (2014). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*. London: Kogan Page.

How your board can influence culture and risk appetite - PWC. (2017). Retrieved from https://www.pwc.dk/da/publikationer/2017/pwc-how-your-board-can-influence-culture-and-risk-appetite.pdf

Harris, S., & Maymí, F. (2016). *CISSP All-in-One Exam Guide*. New York: McGraw-Hill Education.

Hillson D. A. & Murray Webster R. (2012). "A short guide to risk appetite". Aldershot, UK: Gower.

ISACA, (2013). Glossary, Risk Appetite, www.isaca.org/glossary

Landoll, D. J. (2011). *The Security Risk Assessment Handbook a Complete Guide for Performing Security Risk Assessments*. Boca Raton: CRC Press.

L. Rittenberg and F. Martens (2012). Enterprise Risk Management: Understanding and Communicating Risk Appetite. Research commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved.

Maheswari, J. P. (2019, April 23). Breaking the curse of small datasets in Machine Learning: Part 1. Retrieved from https://towardsdatascience.com/breaking-the-curse-of-small-datasets-in-machine-learning-part-1-36f28b0c044d.

McKay, S. M. (2013). *Risk assessment for mid-sized organisations: COSO tools for a tailored approach*. New York: AICPA.

Rittenberg, L., & Martens, F. (2012). Understanding and Communicating Risk Appetite. Committe of Sponsoring Organizations of the Treadway Commission (COSO). Retrieved January 9, 2016, from http://www.coso.org/documents/ERMUnderstanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf

Risk Governance: Appetite, Culture and the Limits of Limits 11/14/2012 Michael Alix, Senior Vice President (Head of the Cross-Firm Perspectives and Analytics (CFPA) function in the Financial Institution Supervision Group at the Federal Reserve Bank of New York.) Remarks at the Risk USA 2012 Conference, New York City • https://www.newyorkfed.org/newsevents/speeches/2012/alix121114

Smart, A., & Creelman, J. (2013). Risk-based performance management: Integrating strategy and risk management. Houndmills, Basingstoke,

Hampshire: Palgrave Macmillan.

Susanto, A. B., & Susanto, P. (2013). The dragon network inside stories of the most successful Chinese family businesses. Singapore: Bloomberg

Thomas C. The impact of poor data quality on the typical enterprise. Communications of the ACM, 41(2):79–82, 1998.

Tom, A. (2018, January 30). Risk Threshold. Retrieved from https://project-management-knowledge.com/definitions/r/risk-threshold/

(Tutorial) Support Vector Machines (SVM) in Scikit-learn. (n.d.). Retrieved from https://www.datacamp.com/community/tutorials/svm-classification-scikit-learn-pythons

Tipton, H. F., & Krause, M. (2010). *Information security management handbook*. Boca Raton: CRC Press.

Young, B., & Coleman, R. (2009). Operational risk assessment: The commercial imperative of a more forensic approach. Hoboken, NJ: Wiley.

Appendix 1

```
#Model 1 (Risk appetite based on the total risk and the sector's risk)
# Importing Data analysis libraries
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
from matplotlib import style
style.use("ggplot")
from sklearn import svm
# Importing the dataset
dataset =
pd.read_excel(r'C:\Users\jussi\PycharmProjects\Thesis\PriscaData.xlsx')
# printing the dataset
print('dataset')
# converting the data set to an array
a =np.array(dataset)
# Taking all the last column(risk appetite) of each row.
# This will serve as the output
y = a[:, 9]
# joining the total risk and sector risk to form a new dataset called x
x = np.column_stack((dataset.Total_Risk, dataset.Sector_Risk))
# Print the x and y
print (x),(y)
#

clf = svm.SVC(C=1000, tol=1e-10, cache_size=600, kernel='linear', gamma= 1e-
8)
# fitting x samples and y classes
clf.fit(x,y)
# summary of the model
print(clf.fit(x,y))
# predicting the risk appetite based on the total risk and sector risk
print(clf.predict([[0.34, 0.03]]))

print(clf.predict([[0.32, 0.03]]))
# new predictions after secotor's updates
print(clf.predict([[0.57, 0.03]]))

print('new prediction')
print(clf.predict([[0.20, 0.03]]))



# Hyperplane coefficient
w = clf.coef_[0]
print(w)
# gradient useful for drawing
g = -w[0] / w[1]
```

```
#
xx = np.linspace(0,1)
yy = g * xx - clf.intercept_[0] / w[1]
# specifying the x and y axis, color and label
h0 = plt.plot(xx, yy, 'k-', label="Risk Appetite by Sector's Risk")
# Draw a scatter plot the is and 2nd x values
plt.scatter(x[:, 0], x[:, 1], c = y)
# Distinguish the risk appetite
plt.legend()
# Distinguish the risk appetite

plt.xlabel(' Total Risk')
plt.ylabel('Sector Risk')
plt.legend()
#Show the graph
plt.show()
```

……

```
# Model 2 (Risk Appetite based on the total risk and geographical location)
# Importing Data analysis libraries
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
from matplotlib import style
style.use("ggplot")
from sklearn import svm
# Importing the dataset
dataset =
pd.read_excel(r'C:\Users\jussi\PycharmProjects\Thesis\PriscaData.xlsx')
# printing the dataset
print('dataset')
# converting the data set to an array
a =np.array(dataset)
# Taking all the last column(risk appetite) of each row.
# This will serve as the output
y = a[:, 9]
# joining the total risk and sector risk to form a new dataset called x
x = np.column_stack((dataset.Total_Risk, dataset.Geographical_Risk))
# Print the x and y
print (x),(y)
#

clf = svm.SVC(C=1000, tol=1e-10, cache_size=600, kernel='linear', gamma= 1e-
8)
# fitting x samples and y classes
clf.fit(x,y)
# summary of the model
print(clf.fit(x,y))
```

```
# predicting the risk appetite based on the total risk and geographical
location risk
print(clf.predict([[0.52, 0.01]]))


# new predictions after  updates geographical location risk updates
print(clf.predict([[0.35, 0.04]]))


# Hyperplane coefficient
w = clf.coef_[0]
print(w)
# gradient useful for drawing
g = -w[0] / w[1]

#
xx = np.linspace(0,1)
yy = g * xx - clf.intercept_[0] / w[1]
# specifying the x and y axis, color and label
h0 = plt.plot(xx, yy, 'k-', label="Risk Appetite by Geographical Location
Risk")
# Draw a scatter plot the ist and 2nd x values
plt.scatter(x[:, 0], x[:, 1], c = y)
# Distinguish the risk appetite

plt.xlabel(' Total Risk')
plt.ylabel('Risk due Geographical Location')
plt.legend()
#Show the graph
plt.show()
```